REMARKS

Upon entry of this amendment, claims 1, 3, 5-7, 10, 12, 13, 18, 20, 21, 23-27, 29, 34 and 36-43 are all the claims pending in the application. Claims 2, 4, 8, 9, 11, 14-17, 19, 22, 28, 30, 31 and 35 have been canceled by this amendment, and claims 36-43 have been added as new claims. No new matter has been added.

I. Claim Rejections

A. Claims 1, 2, 7, 13, 26, 27 and 34 were rejected under 35 U.S.C. § 102(b) as being anticipated by DeBellis (U.S. 6,104,810); and claims 3-5, 10, 11, 18-20, 23, 25, 29 and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis in view of Geiringer (WO 01/93013).

By this amendment, Applicants note that the features recited in claim 4 have been substantially incorporated into claim 1 (with minor changes having been made to the features previously recited in claim 4 which have been incorporated into claim 1).

In particular, Applicants note that claim 1 now recites the feature of an updating unit that is operable to update the parameter stored in the storage unit, wherein the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and wherein the updating unit increases the number of the terms whose coefficients indicate 1 every passage of a predetermined amount of time. Applicants respectfully submit that DeBellis and Geiringer do not teach or suggest such features.

In particular, regarding Geiringer, Applicants note that this reference discloses an encryption method in which a "coefficient may be adjusted by adding to it or subtracting from it an integral value (emphasis added) (see page 3, line 14). Thus, in Geiringer, while a coefficient can be varied, Applicants respectfully submit that Geiringer does not disclose or suggest that the number of terms whose coefficients indicate 1 are increased every passage of a predetermined amount of time.

Further, Applicants respectfully submit that DeBellis does not cure this deficiency of Geiringer. In particular, regarding DeBellis, it is noted that while this reference discloses the ability to periodically backup hardware information to nonvolatile storage (see col. 5, lines 41-43), Applicants respectfully submit that even if DeBellis and Geiringer are considered together, that there is no teaching or suggestion of increasing the number of the terms whose coefficients indicate 1 every passage of a predetermined amount of time, as recited in amended claim 1.

In view of the foregoing, Applicants respectfully submit that the combination of DeBellis and Geiringer do not disclose, suggest or otherwise render obvious all of the features recited in amended claim 1. Accordingly, Applicants submit that claim 1 is patentable over the cited prior art, an indication of which is kindly requested.

Claims 3, 5, 7, 10 and 13 depend from claim 1 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 18, Applicants note that this claim has been amended to recite that the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, wherein the updating unit increases the number of the terms whose coefficients indicate 1 every passage of a predetermined amount of time.

For at least similar reasons as discussed above with respect to claim 1, Applicants submit that the combination of DeBellis and Geiringer does not disclose, suggest or otherwise render obvious such a feature. Accordingly, Applicants submit that claim 18 is patentable over the cited prior art, an indication of which is kindly requested. Claims 20, 23 and 25 depend from claim 18 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 26 and 34, Applicants note that each of these claims has been amended so as to recite the feature of an updating step of updating the parameter, wherein the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and wherein, in the updating step, the number of the terms whose coefficients indicate 1 is increased every passage of a predetermined amount of time.

For at least similar reasons as discussed above with respect to claim 1, Applicants submit that the combination of DeBellis and Geiringer does not disclose, suggest or otherwise render obvious such a feature. Accordingly, Applicants submit that claims 26 and 34 are patentable over DeBellis, an indication of which is kindly requested. Claim 27 and 29 depend from claim 26 and are therefore considered patentable at least by virtue of their dependency.

B. Claims 14, 17, 31 and 35 were rejected under 35 U.S.C. § 102(b) as being anticipated by Geiringer (WO 01/93013). Without acquiescing to this rejection, Applicants note that claims

14, 17, 31 and 35 have been canceled by this amendment, thereby rendering the above-noted rejection moot.

C. Claims 8, 9, 22 and 28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Nishio et al. (U.S. 5,848,154). Without acquiescing to this rejection, Applicants note that claims 8, 9, 22 and 28 have been canceled by this amendment, thereby rendering the above-noted rejection moot.

D. Claims 15 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Geiringer (WO 01/93013) in view of Nishio et al. (U.S. 5,848,154). Without acquiescing to this rejection, Applicants note that claims 15 and 16 have been canceled by this amendment, thereby rendering the above-noted rejection moot.

E. Claims 6, 21 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Geiringer (WO 01/93013) and further in view of Nishio et al. (U.S. 5,848,154).

Claim 6 depends from claim 1, and claims 21 and 24 depend from claim 18. Applicants respectfully submit that Nishio does not cure the deficiencies of DeBellis as Geiringer, as noted above, with respect to claims 1 and 18. Accordingly, Applicants submit that claims 6, 21 and 24 are patentable at least by virtue of their dependency.

F. Claim 12 was rejected under 35 U.S.C. § 103(a) as being unpatentable over DeBellis et al. (U.S. 6,104,810) in view of Geiringer (WO 01/93013), and further in view of Whyte ("Analysis of NTRUEncrypt Paddings, STRONG security that fits everywhere," NTRU, August 2002).

Claim 12 depends from claim 1. Applicants respectfully submit that Whyte does not cure the deficiencies of DeBellis and Geiringer, as noted above, with respect to claim 1. Accordingly, Applicants submit that claim 12 is patentable at least by virtue of its dependency.

II. New Claims

Claims 36-43 have been added as new claims. Claims 36 and 37 depend from claim 1; claims 38 and 39 depend from claim 18; claims 40 and 41 depend from claim 26; and claims 42 and 43 depend from claim 34. Accordingly, Applicants respectfully submit that claims 36-43 are patentable at least by virtue of their dependency.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Masato YAMAMICHI et al.

By: Kenneth W Fields
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/ra
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 20, 2007